Claims

What Is Claimed Is:

1. A method for dynamically creating security keys for a subscriber having at least one preexisting security credential set having at least one pre-existing cryptographic security key, comprising the steps of:

providing a configurable security key manifest operative to contain a non-prespecified number of security keys; and

dynamically controlling, through a configured security key manifest, the generation of at least one new security key for a subscriber based on the received key attribute data contained in the configured security key manifest.

2. The method of claim 1 including the step of generating a new public key pair for the subscriber based on content of the configurable security key manifest.

3. The method of claim 1 including the step of receiving data representing desired new key attribute data by presenting a configurable security key manifest template and receiving new key attribute data through the configurable security key manifest template.

4. The method of claim 1 wherein the step of providing the configurable security key manifest operative to contain a non-prespecified number of security keys includes storing a configured security key manifest for push based or pull based access by the subscriber.

5. The method of claim 1 wherein the configured security key manifest includes updated data representing at least one of: key size, key usage, key maintenance attributes, cryptographic algorithm used, subscriber identification data and authentication data.

6. The method of claim 1 including the steps of:

generating an updated security key manifest as the configured security key manifest to contain data representing at least one of: key size, key usage, key maintenance attributes, cryptographic algorithm used, subscriber identification data and authentication data, for the at least one subscriber; and

comparing the updated security key manifest to the pre-existing credential set containing at least one pre-existing cryptographic security key; and

updating the pre-existing credential set based on the comparison.

7. The method of claim 6 wherein the step of updating the pre-existing credential set includes the step of generating a new public key pair for the subscriber based on content of the configurable security key manifest.

8. The method of claim 1 including the steps of:

generating at least one new key pair in response to content of the configured security key manifest;

continuously analyzing the configured security key manifest content, prior to using a security key pair to determine the suitable security keys necessary for a given operation.

9. The method of claim 1 including the steps of:

digitally signing the configured security key manifest by a trusted key manifest generator;

receiving the digitally signed configured security key manifest;

obtaining the pre-existing credential set; and

prior to analyzing content of the configured security key manifest, verifying the digital signature of the digitally signed configured security key manifest.

10. The method of claim 6 wherein the step of comparing includes determining a difference in security key information between the updated security key manifest and the

pre-existing cryptographic security key.

11. The method of claim 1 wherein the security key is a key pair and wherein the step of dynamically controlling the generation of the at least one security key includes dynamically controlling the number of key pairs for a subscriber in response to content of the configured security key manifest.

12. The method of claim 6 wherein the step of updating the pre-existing credential set includes generating digitally signed data structures corresponding to at least one of a newly generated public key pair.

13. The method of claim 1 wherein the at least one new security key is a symmetric key.

14. The method of claim 3 wherein the data representing desired new key attribute data includes data representing at least one of : key size, key usage, key maintenance attributes, cryptographic algorithm used, subscriber identification data, authentication data.

15. A method for dynamically creating security keys for a subscriber having at least one preexisting security credential set having at least one pre-existing cryptographic security key, comprising the steps of:

providing a configurable security key manifest (table) operative to contain a non-prespecified number of security keys;

receiving, in response to providing the configurable security key manifest, data representing desired new key attribute data by presenting a configurable security key manifest template and receiving new key attribute data through the configurable security key manifest template;

dynamically controlling, through a configured security key manifest, the generation of at least one new security key for a subscriber based on the received key attribute data, wherein the configured security key manifest is an updated security key manifest containing data representing at least one of: key size, key usage, key maintenance attributes, cryptographic algorithm used, subscriber identification data and authentication data;

comparing, by the subscriber, the updated security key manifest to the pre-existing credential set containing at least one of: key size data, cryptographic algorithm designation data, key attribute data and key usage data for, and

updating, by the subscriber, the pre-existing credential set based on the comparison by generating at least one new key for the subscriber based on content of the configurable security key manifest.

16. The method of claim 15 wherein the step of providing the configurable security key manifest operative to contain a non-prespecified number of security keys includes storing the configured security key manifest for push based or pull based access by the subscriber.

17. The method of claim 16 wherein the step of updating the pre-existing credential set includes the step of generating a new public key pair for the subscriber based on content of the configurable security key manifest.

18. The method of claim 15 including the steps of:

generating at least one new key pair in response to content of the configured security key manifest; and

continuously analyzing the configured security key manifest content, prior to using a security key pair to determine the suitable security keys necessary for a given operation.

B1 cont

19. The method of claim 15 including the steps of:

digitally signing the configured security key manifest by a trusted key manifest generator;

receiving, by the subscriber, the digitally signed configured security key manifest;

obtaining, by the subscriber, the pre-existing credential set; and

prior to analyzing content of the configured security key manifest, verifying, by the subscriber, the digital signature of the digitally signed configured security key manifest.

20. The method of claim 15 wherein the step of comparing includes determining a difference in security key information between the updated security key manifest and the pre-existing key data.

21. The method of claim 15 wherein the security key is a key pair and wherein the step of dynamically controlling the generation of the at least one security key includes dynamically controlling the number of key pairs for a subscriber in response to content of the configured security key manifest.

22. The method of claim 15 wherein the step of updating the pre-existing credential set includes generating digitally signed data structures corresponding to at least one of a newly generated public key pair.

23. The method of claim 15 wherein the at least one new security key is a symmetric key.

24. The method of claim 15 wherein the data representing desired new key attribute data includes data representing at least one of : key size, key usage, key maintenance attributes, cryptographic algorithm used, subscriber identification data, authentication data.

25. An apparatus for facilitating dynamic creation of security keys for a subscriber having at least one preexisting security credential set having at least one pre-existing cryptographic security key, comprising:

at least one security key manifest analyzer operative to receive the at least one preexisting security credential set and operative to process a configured security key manifest; and

at least one security credential set generator operative to dynamically generate, from the configured security key manifest, at least one new security key for a subscriber based on received key attribute data contained in the configured security key manifest.

26. The apparatus of claim 25 including a cryptographic key generator operative to generate a new public key pair for the subscriber based on content of the configured security key manifest.

27. The apparatus of claim 25 wherein the security key manifest analyzer compares an updated security key manifest to the pre-existing credential set containing at least one pre-existing cryptographic security key; and wherein the at least one security credential set generator facilitates updating of the pre-existing credential set based on the comparison.

28. The apparatus of 27 wherein the at least one security credential set generator generates a new public key pair for the subscriber based on content of the configured security key manifest.

29. The apparatus of claim 25 wherein the security key analyzer continuously analyzes the configured security key manifest content and wherein the key manifest analyzer is used to determine the suitable security keys necessary for a given operation.

30. The apparatus of claim 25 wherein the security key manifest analyzer receives the digitally signed configured security key manifest, obtains the pre-existing credential set;

and prior to analyzing content of the configured security key manifest, verifying the digital signature of the digitally signed configured security key manifest.

31. The apparatus of claim 30 wherein the key manifest analyzer determines a difference in security key information between the updated security key manifest and the pre-existing key data.

32. The apparatus of claim 25 wherein the security key is a key pair and wherein the security credential generator generates a number of key pairs for a subscriber in response to content of the configured security key manifest.

33. The apparatus of claim 27 wherein the step of updating the pre-existing credential set includes generating digitally signed data structures corresponding to at least one of a newly generated public key pair.

34. The apparatus of claim 25 wherein the at least one new security key is a symmetric key.

35. The apparatus of claim 25 wherein the data representing desired new key attribute data includes data representing at least one of : key size, key usage, key maintenance attributes, cryptographic algorithm used, subscriber identification data, authentication data.

36. An apparatus for facilitating dynamic creation of security keys for a subscriber having at least one preexisting security credential set having at least one pre-existing cryptographic security key, comprising:

at least one key manifest generator that provides the configurable security key manifest operative to contain a non-prespecified number of security keys,

wherein the key manifest generator receives data representing desired new key attribute data by presenting a configurable security key manifest template and receiving new key attribute data through the configurable security key manifest template.

37. The apparatus of claim 36 including storage operative for storing a configured security key manifest for push based or pull based access by the subscriber.

38. The apparatus of claim 36 wherein the configured security key manifest includes updated data representing at least one of: key size, key usage, key maintenance attributes, cryptographic algorithm used, subscriber identification data and authentication data.

39. The apparatus of claim 36 including a trusted key manifest generator operatively responsive to digitally sign the configured security key manifest by;

40. The apparatus of claim 36 including at least one security key manifest analyzer operative to receive the at least one preexisting security credential set and operative to process a configured security key manifest; and

at least one security credential set generator operative to dynamically generate, from the configured security key manifest, at least one new security key for a subscriber based on received key attribute data contained in the configured security key manifest.

41. The apparatus of claim 40 including a cryptographic key generator operative to generate a new public key pair for the subscriber based on content of the configured security key manifest.

42. The apparatus of claim 40 wherein the security key manifest analyzer compares an updated security key manifest to the pre-existing credential set containing at least one pre-existing cryptographic security key; and wherein the at least one security credential set generator facilitates updating of the pre-existing credential set based on the comparison.

B1 cont

43. The apparatus of 42 wherein the at least one security credential set generator generates a new public key pair for the subscriber based on content of the configured security key manifest.

44. A method for dynamically creating security keys for a subscriber comprising the steps of:

providing a configurable security key manifest operative to contain a non-pre-specified number of security keys; and

dynamically controlling, through a configured security key manifest, initial generation of at least one security key for the subscriber, based on received key attribute data contained in the configured secured key manifest.

45. The method of claim 44 including the step of generating a new public key pair for the subscriber based on content of the configurable security key manifest.

46. The method of claim 44 including the step of receiving data representing desired new key attribute data by presenting a configurable security key manifest template and receiving new key attribute data through the configurable security key manifest template.

47. The method of claim 44 wherein the step of providing the configurable security key manifest operative to contain a non-prespecified number of security keys includes storing a configured security key manifest for push based or pull based access by the subscriber.

48. The method of claim 44 wherein the configured security key manifest includes updated data representing at least one of: key size, key usage, key maintenance attributes, cryptographic algorithm used, subscriber identification data and authentication data.